Amendments to the Claims

1. (Currently Amended) A method of processing a message for authentication, said method comprising:

determining whether said message fits within an input block of a compression function;

performing a single iteration of ~~a~~ the compression function using a key and said message as inputs when said message fits within an input block of said compression function and using a result from said compression function without further iteration thereof to produce a message authentication code; and

using a hash function nested within a keyed hash function to process said message when said message does not fit within an input block of said compression function, and using a result from said keyed hash function to produce a message authentication code.

2. (Original) The method of claim **1** wherein said step of using comprises the steps of:

providing a first portion and a second portion of said message;

performing a hash function using said first portion as an input to achieve a result; and

performing a keyed hash function using said second portion and said result as inputs.

3. (Original) The method of claim **2** wherein said hash function is an iterated hash function F and said keyed hash function is a keyed compression function f.

4. (Original) The method of claim **2** wherein said hash function is an iterated hash function F and said keyed hash function is an iterated hash function F.

5. (Cancelled)

6. (Cancelled)

7. (Currently Amended) A method of processing a message for authentication, said method comprising:

providing a first portion and a second portion of said message;

performing a hash function using said first portion as an input to achieve a result; and

performing a keyed hash function using a concatenation of said second portion and said result as inputs.

8. (Original) The method of claim **7** comprising the step of:

determining whether said message fits within an input block of a compression function; and

performing said steps of providing, performing and performing when said message does not fit within an input block of said compression function.

9. (Original) The method of claim **7** comprising the step of:

determining whether said message fits within an input block of a compression function; and

performing a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function.

10. (Original) The method of claim **7** wherein said hash function is an iterated hash function F and said keyed hash function is a keyed compression function f.

11. (Original) The method of claim **7** wherein said hash function is an iterated hash function F and said keyed hash function is an iterated hash function F.

12. (Cancelled)

13. (Cancelled)

14. (Currently Amended) A message authentication system comprising:

processing circuitry configured to determine whether a message fits within an input block of a compression function; and

processing circuitry configured to perform a ~~single iteration of a~~ compression function using a key and said message as inputs, and to output a message authentication code after a single iteration of the compression function in the event that ~~when said~~the message fits within ~~an input~~one said block ~~of said compression function and~~, but to use a hash function nested within a keyed hash function to process said message when said message does not fit within ~~an input~~ one said block ~~of said compression function.~~.

15. (Cancelled)

16. (Currently Amended) A message authentication system comprising:

processing circuitry configured to provide a first portion and a second portion of ~~said~~ a message, perform a hash function using said first portion as an input to achieve a result, and perform a keyed hash function using a concatenation of said second portion and said result as inputs.

17. (Cancelled)

18. (Cancelled)

19. (New) A method of processing a message x for authentication, comprising:

(a) conditionally processing x to provide an intermediate result y;

(b) compressing x or y with a keyed compression function having a block size; and

(c) providing a result of the compressing step for use in a message authentication scheme,

wherein (a) comprises using a hash function to compress at least a portion of x and is carried out on condition that x exceeds the block size.

20. (New) The method of claim **19** wherein (a) comprises providing a first portion and a second portion of the message x, performing a hash function using the first portion as an input to achieve a result; and concatenating the result with the second portion.

21. (New) A message authentication system comprising:

processing circuitry configured to determine whether a message x is larger than an input block size b of a keyed compression function;

processing circuitry configured to apply a hash function to compress at least a portion of x, thereby to provide an intermediate result y, said processing circuitry to be activated only in the event that x is larger than b; and

processing circuitry configured to compress x or y with said keyed compression function, thereby to provide a result for use in a message authentication scheme.